

AMENDMENT

In the Specification

Please replace the paragraph starting at page 1, line 18 with the following:

a' The subject matter of this application is related to the subject matter in a co-pending non-provisional application by the same inventor as the instant application entitled, "Method and Apparatus for Facilitating Single Sign On through Redirection to a Login Server," having serial number 09/550,725, and filing date 17 April 2000 (Attorney Docket No. OR99-17601).

Please replace the paragraph starting at page 8, line 10 with the following:

a2 Client 101 includes browser 130. Browser 130 can include any type of web browser capable of viewing a web site, such as the INTERNET EXPLORER™ browser distributed by the Microsoft Corporation of Redmond, Washington.

In the Claims:

- a3
- 1 1. (Unchanged) A method for facilitating access to a plurality of
 - 2 applications that require passwords, comprising:
 - 3 receiving a request for a password from an application running on a
 - 4 remote computer system, the request being received at a local computer system;
 - 5 authenticating the request as originating from a trusted source;
 - 6 using an identifier for the application to look up the password for the
 - 7 application in a password store containing a plurality of passwords associated with
 - 8 the plurality of applications; and

9 if the password exists in the password store, sending the password or a
10 function of the password to the application on the remote computer system.

1 2. (Unchanged) The method of claim 1, wherein the request for the
2 password includes computer code that when run on the local computer system
3 requests the password on behalf of the application on the remote computer system.

1 3. (Unchanged) The method of claim 2, wherein the computer code is in
2 the form of a JAVA applet that runs on a JAVA virtual machine on the local
3 computer system.

1 4. (Unchanged) The method of claim 3, wherein sending the password or
2 the function of the password to the application to the remote computer system
3 involves:
4 communicating the password to the JAVA applet; and
5 allowing the JAVA applet to forward the password to the application on
6 the remote computer system.

1 5. (Unchanged) The method of claim 3, wherein the JAVA applet is a
2 signed JAVA applet, and wherein authenticating the request includes
3 authenticating the JAVA applet's certificate chain.

1 6. (Unchanged) The method of claim 1, wherein authenticating the
2 request involves authenticating a creator of the request.

1 7. (Unchanged) The method of claim 1, wherein authenticating the
2 request involves authenticating the remote computer system that sent the request.

1 8. (Unchanged) The method of claim 1, further comprising, if the
2 password store is being accessed for the first time,
3 prompting a user for a single sign on password for the password store; and
4 using the single sign on password to open the password store.

1 9. (Unchanged) The method of claim 8, wherein if a time out period for
2 the password store expires,
3 prompting the user again for the single sign on password for the password
4 store; and
5 using the single sign on password to open the password store.

1 10. (Unchanged) The method of claim 1, wherein if the password store is
2 being accessed for the first time, the method further comprises authenticating the
3 user through an authentication mechanism, wherein the authentication mechanism
4 can include:
5 a smart card;
6 a biometric authentication mechanism; and
7 a public key infrastructure.

1 11. (Unchanged) The method of claim 1, wherein if the password does
2 not exist in the password store, the method further comprises:
3 adding the password to the password store; and
4 sending the password to the application on the remote computer system.

1 12. (Unchanged) The method of claim 11, wherein adding the password
2 to the password store further comprises automatically generating the password.

1 13. (Unchanged) The method of claim 11, wherein adding the password
2 to the password store further comprises asking a user to provide the password.

1 14. (Unchanged) The method of claim 1, further comprising decrypting
2 data in the password store prior to looking up the password in the password store.

1 15. (Unchanged) The method of claim 1, wherein the password store is
2 located on a second remote computer system.

1 16. (Once Amended) The method of claim 1, wherein the password store
2 is located on one of:
3 a local smart card;
4 a removable storage medium; and
5 a memory button.

1 17. (Unchanged) The method of claim 1, further comprising:
2 receiving a request to change the password from the application on the
3 remote computer system;
4 automatically generating a replacement password;
5 storing the replacement password in the password store; and
6 forwarding the replacement password or the password function to the
7 application on the remote computer system.

1 18. (Unchanged) A computer-readable storage medium storing
2 instructions that when executed by a computer cause the computer to perform a
3 method for facilitating access to a plurality of applications that require passwords,
4 the method comprising:

5 receiving a request for a password from an application running on a
6 remote computer system, the request being received at a local computer system;
7 authenticating the request as originating from a trusted source;
8 using an identifier for the application to look up the password for the
9 application in a password store containing a plurality of passwords associated with
10 the plurality of applications; and
11 if the password exists in the password store, sending the password or a
12 function of the password to the application on the remote computer system.

1 19. (Unchanged) The computer-readable storage medium of claim 18,
2 wherein the request for the password includes computer code that when run on the
3 local computer system requests the password on behalf of the application on the
4 remote computer system.

1 20. (Unchanged) The computer-readable storage medium of claim 19,
2 wherein the computer code is in the form of a JAVA applet that runs on a JAVA
3 virtual machine on the local computer system.

1 21. (Unchanged) The computer-readable storage medium of claim 20,
2 wherein sending the password or the function of the password to the application to
3 the remote computer system involves:
4 communicating the password to the JAVA applet; and
5 allowing the JAVA applet to forward the password to the application on
6 the remote computer system.

1 22. (Unchanged) The computer-readable storage medium of claim 20,
2 wherein the JAVA applet is a signed JAVA applet, and wherein authenticating the
3 request includes authenticating the JAVA applet's certificate chain.

1 23. (Unchanged) The computer-readable storage medium of claim 18,
2 wherein authenticating the request involves authenticating a creator of the request.

1 24. (Unchanged) The computer-readable storage medium of claim 18,
2 wherein authenticating the request involves authenticating the remote computer
3 system that sent the request.

1 25. (Unchanged) The computer-readable storage medium of claim 18,
2 wherein the method further comprises, if the password store is being accessed for
3 the first time,
4 prompting a user for a single sign on password for the password store; and
5 using the single sign on password to open the password store.

1 26. (Unchanged) The computer-readable storage medium of claim 25,
2 wherein if a time out period for the password store expires, the method further
3 comprises:
4 prompting the user again for the single sign on password for the password
5 store; and
6 using the single sign on password to open the password store.

1 27. (Unchanged) The computer-readable storage medium of claim 18,
2 wherein if the password store is being accessed for the first time, the method
3 further comprises authenticating the user through an authentication mechanism,
4 wherein the authentication mechanism can include:
5 a smart card;
6 a biometric authentication mechanism; and
7 a public key infrastructure.

1 28. (Unchanged) The computer-readable storage medium of claim 18,
2 wherein if the password does not exist in the password store, the method further
3 comprises:
4 adding the password to the password store; and
5 sending the password to the application on the remote computer system.

1 29. (Unchanged) The computer-readable storage medium of claim 28,
2 wherein adding the password to the password store further comprises
3 automatically generating the password.

1 30. (Unchanged) The computer-readable storage medium of claim 28,
2 wherein adding the password to the password store further comprises asking a
3 user to provide the password.

1 31. (Unchanged) The computer-readable storage medium of claim 18,
2 wherein the method further comprises decrypting data in the password store prior
3 to looking up the password in the password store.

1 32. (Unchanged) The computer-readable storage medium of claim 18,
2 wherein the password store is located on a second remote computer system.

1 33. (Once Amended) The computer readable storage medium of claim
2 18, wherein the password store is located on one of:
3 a local smart card;
4 a removable storage medium; and
5 a memory button.

1 34. The computer-readable storage medium of claim 18, wherein the
2 method further comprises:
3 receiving a request to change the password from the application on the
4 remote computer system;
5 automatically generating a replacement password;
6 storing the replacement password in the password store; and
7 forwarding the replacement password or the password function to the
8 application on the remote computer system.

1 35. (Unchanged) An apparatus that facilitates accessing a plurality of
2 applications that require passwords, comprising:
3 a receiving mechanism that receives a request for a password from an
4 application running on a remote computer system, the request being received at a
5 local computer system;
6 an authentication mechanism that authenticates the request as originating
7 from a trusted source;
8 a lookup mechanism that uses an identifier for the application to look up
9 the password for the application in a password store containing a plurality of
10 passwords associated with the plurality of applications; and
11 a forwarding mechanism that sends the password to the application on the
12 remote computer system if the password exists in the password store.

1 36. (Unchanged) The apparatus of claim 35, wherein the request for the
2 password includes computer code that when run on the local computer system
3 requests the password on behalf of the application on the remote computer system.

1 37. (Unchanged) The apparatus of claim 36, wherein the computer code
2 is in the form of a JAVA applet that runs on a JAVA virtual machine on the local
3 computer system.

1 38. (Unchanged) The apparatus of claim 37, wherein the forwarding
2 mechanism is configured to send the password to the application on the remote
3 computer system by:
4 communicating the password to the JAVA applet; and
5 allowing the JAVA applet to forward the password to the application on
6 the remote computer system.

A3
1 39. (Unchanged) The apparatus of claim 37, wherein the JAVA applet is
2 a signed JAVA applet, and wherein the authentication mechanism is configured to
3 authenticate a certificate chain.

1 40. (Unchanged) The apparatus of claim 35, wherein the authentication
2 mechanism is configured to authenticate a creator of the request.

1 41. (Unchanged) The apparatus of claim 35, wherein the authentication
2 mechanism is configured to authenticate the remote computer system that sent the
3 request.

1 42. (Unchanged) The apparatus of claim 35, wherein if the password
2 store is being accessed for the first time, the lookup mechanism is configured to:
3 prompt a user for a single sign on password for the password store; and to
4 use the single sign on password to open the password store.

1 43. (Unchanged) The apparatus of claim 42, wherein if a time out period
2 for the password store expires, the lookup mechanism is configured to:
3 prompt the user again for the single sign on password for the password
4 store; and to
5 use the single sign on password to open the password store.

1 44. (Unchanged) The apparatus of claim 35, wherein if the password
2 store is being accessed for the first time, the lookup mechanism is configured to
3 authenticate the user through an authentication mechanism, wherein the
4 authentication mechanism can include:
5 a smart card;
6 a biometric authentication mechanism; and
7 a public key infrastructure.

1 45. (Unchanged) The apparatus of claim 35, further comprising an
2 insertion mechanism, wherein if the password does not exist in the password store
3 the insertion mechanism is configured to:
4 add the password to the password store; and to
5 send the password to the application on the remote computer system.

1 46. (Unchanged) The apparatus of claim 45, wherein the insertion
2 mechanism is additionally configured to automatically generate the password.

1 47. (Unchanged) The apparatus of claim 45, wherein the insertion
2 mechanism is additionally configured to ask a user to provide the password.

1 48. (Unchanged) The apparatus of claim 35, further comprising a
2 decryption mechanism that is configured to decrypt data in the password store.

1 49. (Unchanged) The apparatus of claim 35, wherein the password store
2 is located on a second remote computer system.

1 50. (Once Amended) The apparatus of claim 35, wherein the password
2 store is located on one of:
3 a local smart card;
4 a floppy disk; and
5 a memory button.

1 51. (Unchanged) The apparatus of claim 35, further comprising a
2 password changing mechanism that is configured to:
3 receive a request to change the password from the application on the
4 remote computer system;
5 automatically generate a replacement password;
6 store the replacement password in the password store; and to
7 forward the replacement password to the application on the remote
8 computer system.

1 52. (New) A method for facilitating access to a plurality of applications
2 that require passwords, comprising:
3 receiving a request to look up a password at a password server;
4 wherein the request is received from a client and includes an identifier for
5 an application requesting the password from the client;
6 using the identifier for the application to look up the password for the
7 application in a password store containing a plurality of passwords associated with
8 the plurality of applications; and

9 if the password exists in the password store, sending the password or a
10 function of the password to the client, so that the client can present the password
11 to the application.

1 53. (New) The method of claim 53, wherein the request is received from
2 computer code running on the client that requests the password on behalf of the
3 application.

1 54. (New) The method of claim 54, wherein the computer code is in the
2 form of a JAVA applet that runs on a JAVA virtual machine on the client.

1 55. (New) A server that distributes code for facilitating access to a
2 plurality of applications that require passwords, wherein the code operates by:
3 receiving a request for a password from an application running on a
4 remote computer system, the request being received at a local computer system;
5 authenticating the request as originating from a trusted source;
6 using an identifier for the application to look up the password for the
7 application in a password store containing a plurality of passwords associated with
8 the plurality of applications; and
9 if the password exists in the password store, sending the password or a
10 function of the password to the application on the remote computer system.

COMMENTS

Applicant has amended claims 16, 33 and 50, and as added new claims 53-56.